UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00246

ATTACKERS TARGETING MICROSOFT TEAMS W/ TROJANS

DATE ISSUED: 21st February 2022

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	HARD	MEDIUM	**EASY**

OVERVIEW

Attackers are targeting Microsoft's popular collaboration tool Microsoft Teams by planting malicious documents in chat threads containing Trojan malware that when executed can take over user machines as well as exfiltrate information and files.

BREAKDOWN

Microsoft Teams surge in popularity may be partially attributed to the rise in remote working and the need to collaborate with your team online due to the current pandemic situation. Attackers are seizing this as an opportunity to formulate new attacks targeted at the Teams platform as a new attack surface. In this particular attack, Microsoft Office files are being used as the vehicle to distribute malware. The files appear to be legitimate documents and when a user interacts with them, and they execute and run in the background giving attackers the ability to install DLL files allowing the program to "self-administer" in order to take over the devices. This may also lead to supply chain attacks by compromising linked or partner organisations as well as attackers being able to exfiltrate files and listen in on chats. They may also be able to compromise email accounts and other Microsoft Office apps as well once "inside".

REMEDIATION STEPS

- Ensure you have clear electronic communications policies in place to dictate how information/data is to be shared inside your organisation relating to its sensitivity levels.
- Ensure endpoint protections is running on all end-user devices to detect and respond to anomalous system behaviours and known threat signatures.
- Check default Microsoft default security protections and remediate where necessary,
- Ensure administrators have oversight of users adding/inviting persons to you Teams environment and channels and that these abilities are restricted or actively monitored.

REFERENCES & RESOURCES

Avanan https://www.avanan.com/blog/hackers-attach-malicious-.exe-files-to-teams-conversations
Threatpost https://threatpost.com/microsoft-teams-targeted-takeover-trojans/178497/